Physical-Layer Security Over Non-Small-Scale Fading Channels

Peng, gaofeng; Tang, Chaoqing; Zhang, Xv; Li, Tingting; Weng, Ying; Chen, Yunfei

IEEE Transactions on Vehicular Technology

DOI:
10.1109/TVT.2015.2412140

Published: 11/03/2015

Peer reviewed version

Physical-Layer Security over Non-Small Scale Fading Channels

Gaofeng Pan, Chaoqing Tang, Xv Zhang, Tingting Li, Ying Weng, Yunfei Chen

Abstract: In this paper, we propose a comprehensive framework for performance analysis of secure communications over non-small scale fading channels. Considering the three different cases where the main and eavesdropper channels experience independent/correlated log-normal fading, or independent composite fading, we study secrecy capacity and secrecy outage (including the probability of non-zero secrecy capacity and secure outage probability), respectively. The approximated closed-form expressions for secrecy capacity, the probability of non-zero secrecy capacity, and secure outage probability have been derived for these three different types of non-small fading channels, respectively. Finally, the accuracy of our performance analysis is verified by simulation results.

Keywords: Secure capacity, the probability of non-zero secrecy, secure outage probability, log-normal fading, composite fading.

1. Introduction

Nowadays, securing the communication over the wireless channels at the physical layer has attracted considerableattention from researchers due to the inherent openness of communications over wireless channels offerring a shared medium, particularly making it vulnerable to eavesdropping and jamming attacks.

Traditionally, security was regarded as an independent issue beyond the physical layer scale, and was well studied and addressed through designing and implementing some cryptographic algorithms (e.g., the widely-used RSA and Advanced Encryption Standard (AES)). However,all these works were carried on the premise ofholding error-free links in the physical layer. In wireless scenarios, it is expensive to distribute and manage the secret key, and further vulnerable to attacks, due to the broadcast nature of the wireless medium [1]. Thus, researchers turn to physical layer security, and try to provide secure data transmission by exploiting the characteristics of wireless channels.

The eavesdropping attack was first studied by Wyner in [2] where a single-user secure communication setting was considered: a source node (Alice) wished to transmit confidential information to a legitimate destination node (Bob) and keep eavesdropper (Eve) as ignorant of the information as possible, as shown in Fig. 1. While a discrete memoryless wiretap channel was adopted, the level of ignorance at Evewas measured by its equivocation, and the capacity -equivocation region was characterized at the same time. Csiszar and Korner [3] extended Wyner's work to general broadcast channels with confidential messages. Leung-Yan-Cheong and Hellman [4] extendedWyner's result to the Gaussian wiretap channel, and found that the secrecy capacity is the difference between the capacities of the main and the eavesdropper channels. Then the performance measure of interest in wireless secure communications is to find out the secrecy capacity, which is the largest achievable communication rate from the source to the destination while the eavesdropper obtains no information.

Single-antenna wiretap channels were studied in [5-13]. Quasistatic fading channel was

considered while the channel state information (CSI) of the main and the eavesdropper channels was not available at the source, and an alternative definition of outage probability was presented in the view of time, i.e., secure communications could be guaranteed for the fraction of time when the main channel was stronger than the eavesdropper channel [5-7]. Gopala et al. [8] addressed the ergodic secrecy capacity of fading channels, and described an optimal power allocation and a transmission strategy to let messages be transmitted opportunistically while the condition of the main channel instantaneously outperformed that of the eavesdropper channel. Therefore, by making use of the opportunistic transmission in this way, a positive secrecy capacity might be achieved even when the main channel was noisier. Concurrently and independently, some similar results were given in [9] where the secrecy capacity was further investigated over the fading broadcast channel. Khisti et al. [10] extended the work in [3] to the scenario where multiple legitimate receivers existed over the fading channel, and discussed the secrecy capacity in terms of outage probability in the delay limited case.

Multiple-antenna wiretap channels have been studied recently in [11-17]. Liu and Shamai analyzed the secrecy capacity of the 2-2-1 Gaussian Multi-input multi-output (MIMO) wiretap channel consisting of a transmitter and a receiver with two antennas each, and an eavesdropper with a single antenna, and developed a tight upper bound of the secrecy capacity that met the proposed achievable secrecy rate. Khistiand Wornell [13, 14] took account of the Gaussian MIMO wiretap channel to compute the secrecy capacity by exploiting the result in [3], and identified the necessary auxiliary random variables. Furthermore, they maximized the secrecy capacity for MIMO channel through forming a nonconvex problem. Oggier and Hassibi [15] calculated the perfect secrecy capacity of the multiple antenna MIMO broadcast channel where the number of antennas was arbitrary for both the transmitter and the two receivers. The secrecy capacity region of the Gaussian MIMO broadcast channel was discussed in [16]. Considering the practical scenario that no CSI was available at the transmitters, Yang et al. [17] investigated the secrecy performance of MIMO over Nakagami-*m* fading channels while transmit antenna selection was adopted. Closed-form expressions for the probability of non-zero secrecy capacity and the exact secrecy outage probability were derived, based on which the ε-outage secrecy capacity was characterized.

All the above works assumed that the main channel was independent of the eavesdropper channel. In the case of correlated fading channels, Jeon et al. [18] dealt with the asymptotic behavior of the secrecy capacity in the high signal-to-noise ratio (SNR) regime and found that the secrecy capacity converged to an upper-bound while the ergodic capacity of fading channels grew logarithmically with SNR in general. Further, both the average secrecy capacity and the outage probability of secure communications over correlated Rayleigh fading channels were studied in [19].

Obviously, we can find that all the aforementioned works are limited to Gaussian channels [4], [11-16] or small-scale fading channels, e.g. independent/correlated Rayleigh fading channels [5-10], [18-19]and Nakagami-*m* fading channels [17].

In practical wireless environment, amplitude variation of a received radio signal can be modeled as a product of path loss and fading [20]. Several models exist for characterizing path loss, including the variants of Okumura–Hata and Walfisch–Ikegami formulas [21]. Fading may be either due to multipath propagation, referred to as small-scale multipath fading, or due to the shadowing from obstacles affecting the wave propagation, usually referred to as shadow fading.

Multipath fading arises from the constructive and destructive combination of randomly delayed, reflected, scattered and diffracted signal components while shadowing affects the link quality by slow variation of the mean level. Some statistical models have been proposed and well adopted to depict the effect of small-scale fading on wireless communications, e.g., Rayleigh, Rice, and Nagakami-*m*.

In addition to small-scale multipath fading, the quality of the received signals may also be affected by slow variations of the mean signal level due to shadowing from various obstacles in the propagation path. The lognormal distribution is often appropriately used to describe and model statistics of the path gain in midscale fading environments caused by shadowing in outdoor environments. More recently, researchers have approved that the small-scale fading of indoor ultra wideband channels can also be well captured by the log-normal distribution [22].

So far, there has been few works on secure communications over log-normal fading channels [23, 24]. Liu [23] investigated the information theoretic secrecy for the independent log-normal fading channel, and derived the closed-form expressions of the probability of strictly positive secrecy capacity for two types of systems with single eavesdropper and double eavesdroppers, respectively. Zahurul and Ratnarajah [24] studied secrecy capacity for the log-normal fading channel where the main channel was correlated with the eavesdropper channel, and proposed the closed-form analytical expression for the upper bound of secrecy capacity while an optimal power allocation at the transmitter was found to achieve the secrecy capacity.

Furthermore, multipath fading and shadowing occur simultaneously in many cases for communication systems with low mobility or stationary users and certain land-mobile satellite systems.This composite fading environment consists of multipath fading superimposed by log-normal shadowing. To the best of our knowledge, till now, there is no work related to the outage behavior of secure communications in non-small fading environment, namely, over impendent/correlated log-normal channels or composite fading channels.

Motivated by the above observations, we propose a comprehensive framework for performance analysis of secure communications over non-small scale fading channels, including independent/ correlated log-normal fading channels, and independent composite fading channels. The main contributions of our work are listed in terms of performance indices as follows:

(1) Secure Capacity
   a. Differing from the work in [23], we study secrecy capacity over independent log-normal fading channels by employingan approximation method to calculate the expectation of a normally distributed variable's real function, which leads to an approximated analytical expression with low computational complexity as shown in Section 3.1;
   b. We propose the closed-form expression for the secure capacity over correlated log-normal channels;
   c. We study the secure capacity through approximating the generalized-*K* distribution probability density function (pdf) by a log-normal distribution.

(2) Secrecy Outage
   a. The probability of non-zero secrecy capacity is investigated over independent/ correlated log-normal fading channels and composite fading channels, respectively. Furthermore, the approximated closed-form expressions are also derived for these three different types of fading channels, respectively;

b. The secure outage probability is investigated over independent/correlated log-normal fading channels and composite fading channels, respectively. Furthermore, the approximated closed-form expressions are also derived for these three different types of fading channels, respectively.

The rest of this paper is organized as follows. In Section II, we describe the system and signal models considered in our work. We propose the secrecy capacity analysis for the considered three different non-small fading channels in Section III. The secrecy outage analysis is carried out in Section IV. In Section V numerical and simulation results are presented and discussed. Finally, we conclude the paper with some remarks in Section VI.

2. System and signal models

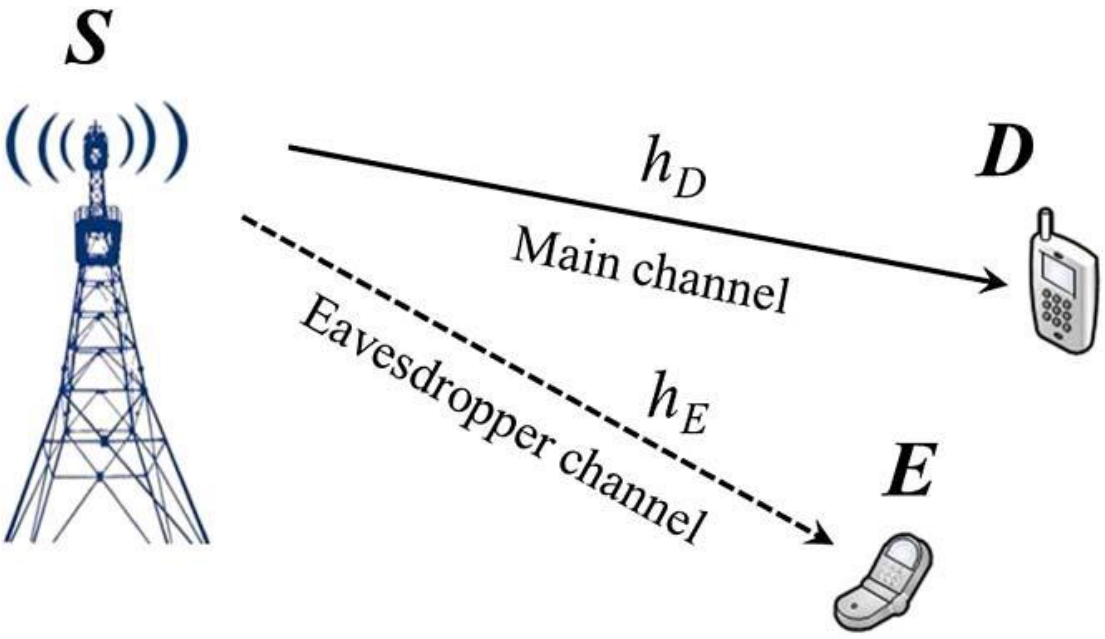

Fig. 1. System model

Suppose that the source *S* sends a message to the legitimate receiver *D*over the main channel while the eavesdropper *E* attempts to decode this message from its received signal through the eavesdropper channel, as shown in Fig. 1. In this paper, we consider the cases where the main and eavesdropper channels experience independent/correlated log-normal fading or independent composite fading. (The correlated fading could happen if *E* is closely located to *D*). We assume that both channels experience the ergodic block fading where channel coefficients remain constants during a block period and vary independently across blocks.Furthermore, we also assume that the full CSI of both the main and eavesdropper channels is available at *S*.

The received signals at *D* and *E* are given respectively by

$$y_D = \sqrt{P_t} h_D x + n_D \tag{1-a}$$

$$y_E = \sqrt{P_t} h_E x + n_E \tag{1-b}$$

where P_t represents the fixed average transmit power, and h_D and h_E are complex channel gains

from S to D (main channel) and E (eavesdropper channel), respectively, and n_D and n_E are independent complex Gaussian noises with zero-mean and unit-variances.

The instantaneous SNRs of the received signals at D and E can be given as $\gamma_D = P_t |h_D|^2$ and $\gamma_E = P_t |h_E|^2$, respectively. Thus, according to [3], the instantaneous secrecy capacity is defined as

$$C_s(\gamma_D, \gamma_E) = \max\{\ln(1+\gamma_D) - \ln(1+\gamma_E), 0\} \quad (2)$$

where $\ln(1+\gamma_D)$ and $\ln(1-\gamma_E)$ are the capacity of the main and channel eavesdropper channels, respectively. Then the average secrecy capacity can be given by [3]

$$\bar{C}_s(\gamma_D, \gamma_E) = E[C_s(\gamma_D, \gamma_E)] = \int_0^\infty \int_0^\infty C_s(\gamma_D, \gamma_E) f(\gamma_D, \gamma_E) d\gamma_D d\gamma_E \quad (3)$$

where $f(\gamma_D, \gamma_E)$ is the joint pdf.

3. Secrecy capacity analysis over non-small scale fading channels

In this section, we present the analysis on the average secrecy capacity over three different types of non-small scale fading channels: independent/correlated log-normal fading channels, and independent composite fading channel.

3.1 Independent log-normal fading

Assume that the main and eavesdropper channels experience independent log-normal fading, namely

$$f(h_i; \mu_i, \sigma_i) = \frac{1}{h_i \sqrt{2\pi\sigma_i^2}} \exp\left(-\frac{(\ln h_i - \mu_i)^2}{2\sigma_i^2} \right), \quad i \in \{D, E\} \quad (4)$$

where μ_i and σ_i are the mean and variance for h_i's natural logarithm, respectively.

Therefore, according to the prosperities of log-normal distribution, we have the instantaneous SNRs of the received signals at D and E, γ_D and γ_E, obey log-normal distribution, that is

$$\gamma_i \sim \log - N(\mu_{\gamma_i}, \sigma_{\gamma_i}^2), \quad i \in \{D, E\} \quad (5)$$

where $\mu_{\gamma_i} = 2\mu_i + \ln P_t$, and $\sigma_{\gamma_i}^2 = 4\sigma_i^2$.

As the main and eavesdropper channels experience independent log-normal fading, using Eq. (5) in Eq. (3), we have

$$\begin{aligned}
&\bar{C}_s(\gamma_D, \gamma_E) = \int_0^\infty \int_0^\infty Cs(\gamma_D, \gamma_E) f(\gamma_D) f(\gamma_E) d\gamma_E d\gamma_D \\
&= \int_0^\infty \int_0^{\gamma_D} C_s(\gamma_D, \gamma_E) f(\gamma_D) f(\gamma_E) d\gamma_E d\gamma_D + \int_0^\infty \int_{\gamma_D}^\infty C_s(\gamma_D, \gamma_E) f(\gamma_D) f(\gamma_E) d\gamma_E d\gamma_D \\
&= \int_0^\infty \int_0^{\gamma_D} [\ln(1+\gamma_D) - \ln(1+\gamma_E)] f(\gamma_D) f(\gamma_E) d\gamma_E d\gamma_D \\
&= \int_0^\infty \int_0^{\gamma_D} \ln(1+\gamma_D) f(\gamma_D) f(\gamma_E) d\gamma_E d\gamma_D - \int_0^\infty \int_0^{\gamma_D} \ln(1+\gamma_E) f(\gamma_D) f(\gamma_E) d\gamma_E d\gamma_D \\
&= \int_0^\infty \ln(1+\gamma_D) f(\gamma_D) \int_0^{\gamma_D} f(\gamma_E) d\gamma_E d\gamma_D - \int_0^\infty \ln(1+\gamma_E) f(\gamma_E) \int_{\gamma_E}^\infty f(\gamma_D) d\gamma_D d\gamma_E \\
&= \int_0^\infty \ln(1+\gamma_D) \Phi\left(\frac{\ln \gamma_D - \mu_{\gamma_E}}{\sigma_{\gamma_E}} \right) f(\gamma_D) d\gamma_D - \int_0^\infty \ln(1+\gamma_E) \left[1 - \Phi\left(\frac{\ln \gamma_E - \mu_{\gamma_D}}{\sigma_{\gamma_D}} \right) \right] f(\gamma_E) d\gamma_E
\end{aligned}$$

$$= \int_0^\infty \ln(1+\gamma_D)\Phi\left(\frac{\ln\gamma_D - \mu_{\gamma_E}}{\sigma_{\gamma_E}}\right) f(\gamma_D)d\gamma_D - \int_0^\infty \ln(1+\gamma_E)Q\left(\frac{\ln\gamma_E - \mu_{\gamma_D}}{\sigma_{\gamma_D}}\right) f(\gamma_E)d\gamma_E \quad (6)$$
$$= \bar{C}_D'(\gamma_D) - \bar{C}_E'(\gamma_E)$$

where $\bar{C}_D'(\gamma_D) = \int_0^\infty \ln(1+\gamma_D)\Phi\left(\frac{\ln\gamma_D - \mu_{\gamma_E}}{\sigma_{\gamma_E}}\right) f(\gamma_D)d\gamma_D$ and

$\bar{C}_E'(\gamma_E) = \int_0^\infty \ln(1+\gamma_E)Q\left(\frac{\ln\gamma_E - \mu_{\gamma_D}}{\sigma_{\gamma_D}}\right) f(\gamma_E)d\gamma_E$.

Let $y = \ln\gamma_D$, we can rewrite $\bar{C}_D'(\gamma_D)$ as follows

$$\bar{C}_D'(\gamma_D) = \int_{-\infty}^\infty \ln(1+\exp(y))\Phi\left(\frac{y - \mu_{\gamma_E}}{\sigma_{\gamma_E}}\right) \cdot \frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}} \exp\left(-\frac{1}{2}\left(\frac{y - \mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)^2\right) dy$$
$$= \int_{-\infty}^\infty \psi_D(y) \cdot \frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}} \exp\left(-\frac{1}{2}\left(\frac{y - \mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)^2\right) dy \quad (7)$$

where $\psi_D(y) = \ln(1+\exp(y))\Phi\left(\frac{y - \mu_{\gamma_E}}{\sigma_{\gamma_E}}\right)$.

Some existed works have proved that log-normal behavior is difficult to deal with [25-28].In this work, we adopt the efficient tool proposed by Holtzmanin [29] to deal with Eq. (7). Taking Eq. (5-7) in [29],we have

If $\psi(x)$ is a real function of x, a normally distributed variable with mean μ_x and variance σ_x^2, namely, $x \sim N(\mu_x, \sigma_x^2)$, then, the expectation of $\psi(x)$ can be approximated in terms of three mass points located at μ_x, $\mu_x + \sqrt{3}\sigma_x$ and $\mu_x - \sqrt{3}\sigma_x$, as follows

$$E[\psi(x)] = \frac{2}{3}\psi(\mu_x) + \frac{1}{6}\psi(\mu_x + \sqrt{3}\sigma_x) + \frac{1}{6}\psi(\mu_x - \sqrt{3}\sigma_x) \quad (8)$$

Thus, making use of Eq. (8), we can obtain the approximation for $\bar{C}_D'(\gamma_D)$ as follows

$$\bar{C}_D'(\gamma_D) \approx \frac{2}{3}\psi_D(\mu_{\gamma_D}) + \frac{1}{6}\psi_D(\mu_{\gamma_D} + \sqrt{3}\sigma_{\gamma_D}) + \frac{1}{6}\psi_D(\mu_{\gamma_D} - \sqrt{3}\sigma_{\gamma_D}) \quad (9)$$

Similarly to the derivation of $\bar{C}_D'(\gamma_D)$, we can have

$$\bar{C}_E'(\gamma_E) \approx \frac{2}{3}\psi_E(\mu_{\gamma_E}) + \frac{1}{6}\psi_E(\mu_{\gamma_E} + \sqrt{3}\sigma_{\gamma_E}) + \frac{1}{6}\psi_E(\mu_{\gamma_E} - \sqrt{3}\sigma_{\gamma_E}) \quad (10)$$

where $\psi_E(x) = \ln(1+\exp(x))Q\left(\frac{x - \mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)$.

Then substituting Eq. (9) and Eq. (10) into Eq. (6), the average secrecy capacity can be

obtained as follows

$$\begin{aligned}\bar{C}_s(\gamma_D,\gamma_E) \approx \frac{2}{3}\left[\psi_D\left(\mu_{\gamma_D}\right)-\psi_E\left(\mu_{\gamma_E}\right)\right]+\frac{1}{6}\left[\psi_D\left(\mu_{\gamma_D}+\sqrt{3}\sigma_{\gamma_D}\right)-\psi_E\left(\mu_{\gamma_E}+\sqrt{3}\sigma_{\gamma_E}\right)\right] \\ +\frac{1}{6}\left[\psi_D\left(\mu_{\gamma_D}-\sqrt{3}\sigma_{\gamma_D}\right)-\psi_E\left(\mu_{\gamma_E}-\sqrt{3}\sigma_{\gamma_E}\right)\right]\end{aligned} \tag{11}$$

3.2 Correlated log-normal fading

Assume that the main and eavesdropper channels experience correlated log-normal fading, which typically occurs in propagation under shadowing and antenna diversity systems, where correlation of the lognormal fading gains is due to bulk geometrical and electromagnetic propagation characteristics experienced by differing propagation paths [30-32].

As suggested by [33], a joint log-normal pdf of γ_D and γ_E can be given by

$$\begin{aligned}p_{\gamma_D,\gamma_E}(\gamma_D,\gamma_E) &= \frac{1}{2\pi\sigma_{\gamma_D}\sigma_{\gamma_E}\sqrt{1-\rho^2}\gamma_D\gamma_E} \\ &\cdot\exp\left\{-\frac{1}{1-\rho^2}\left[\frac{(\ln\gamma_D-\mu_{\gamma_D})^2}{2\sigma_{\gamma_D}^2}+\frac{(\ln\gamma_E-\mu_{\gamma_E})^2}{2\sigma_{\gamma_E}^2}-2\rho\left(\frac{\ln\gamma_D-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)\left(\frac{\ln\gamma_E-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right)\right]\right\}, \\ &\qquad \gamma_D\ge 0 \text{ and } \gamma_E\ge 0, \\ &\qquad -1\le\rho\le 1\end{aligned} \tag{12}$$

where ρ is the correlation coefficient. When $\rho=0$, the two diversity paths are uncorrelated. When positive correlation exists (i.e., $0<\rho\le 1$), if one diversity path is strong, it is likely that the other diversity path is also strong, and vice versa. When negative correlation exists (i.e., $-1\le\rho<0$), if one diversity path is weak, it is likely that the other diversity path is strong, and vice versa.

Using Eq. (12) in Eq. (3), we have

$$\begin{aligned}\bar{C}_s(\gamma_D,\gamma_E) &= \int_0^\infty \ln(1+\gamma_D)\int_0^{\gamma_D} p_{\gamma_D,\gamma_E}(\gamma_D,\gamma_E)d\gamma_E d\gamma_D - \int_0^\infty \ln(1+\gamma_E)\int_{\gamma_E}^\infty p_{\gamma_D,\gamma_E}(\gamma_D,\gamma_E)d\gamma_D d\gamma_E \\ &= D_1 + D_2\end{aligned} \tag{13}$$

After some manipulations, we have

$$\begin{aligned}D_1 &= \int_0^\infty \ln(1+\gamma_D)\int_0^{\gamma_D} p_{\gamma_D,\gamma_E}(\gamma_D,\gamma_E)d\gamma_E d\gamma_D \\ &= \int_0^\infty \ln(1+\gamma_D)\frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}\gamma_D}\exp\left\{-\frac{1}{1-\rho^2}\left(\frac{\ln\gamma_D-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)^2\right\} \\ &\quad\cdot\int_0^{\gamma_D}\frac{1}{\sqrt{2\pi}\sqrt{1-\rho^2}\sigma_{\gamma_E}\gamma_E}\exp\left\{-\frac{1}{1-\rho^2}\left[\left(\frac{\ln\gamma_E-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right)^2-\rho\frac{(\ln\gamma_D-\mu_{\gamma_D})(\ln\gamma_E-\mu_{\gamma_E})}{\sigma_{\gamma_D}\sigma_{\gamma_E}}\right]\right\}d\gamma_E d\gamma_D \\ &= \int_0^\infty \ln(1+\gamma_D)\frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}\gamma_D}\exp\left\{-\left(\frac{\ln\gamma_D-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)^2\right\}\int_0^{\gamma_D}\frac{1}{\sqrt{2\pi}\sqrt{1-\rho^2}\sigma_{\gamma_E}\gamma_E} \\ &\quad\cdot\exp\left\{-\frac{1}{1-\rho^2}\left[\left(\frac{\ln\gamma_E-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right)^2-\rho\frac{(\ln\gamma_D-\mu_{\gamma_D})(\ln\gamma_E-\mu_{\gamma_E})}{\sigma_{\gamma_D}\sigma_{\gamma_E}}+\left(\frac{\rho(\ln\gamma_D-\mu_{\gamma_D})}{\sqrt{2}\sigma_{\gamma_D}}\right)^2\right]\right\}d\gamma_E d\gamma_D\end{aligned}$$

$$= \int_0^{\infty} \ln\left(1+\gamma_D\right) \frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}\gamma_D} \exp\left\{-\left(\frac{\ln\gamma_D - \mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)^2\right\} \int_0^{\gamma_D} \frac{1}{\sqrt{2\pi}\sqrt{1-\rho^2}\sigma_{\gamma_E}\gamma_E}$$

$$\cdot \exp\left\{-\frac{1}{1-\rho^2}\left[\left(\frac{\ln\gamma_E - \mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right) - \left(\frac{\rho\left(\ln\gamma_D - \mu_{\gamma_D}\right)}{\sqrt{2}\sigma_{\gamma_D}}\right)\right]^2\right\} d\gamma_E d\gamma_D$$

$$= \int_0^{\infty} \ln\left(1+\gamma_D\right) \frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}\gamma_D} \exp\left\{-\left(\frac{\ln\gamma_D - \mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)^2\right\}$$

$$\cdot \int_{-\infty}^{\ln\gamma_D} \frac{1}{\sqrt{2\pi}\sqrt{1-\rho^2}\sigma_{\gamma_E}} \exp\left\{-\frac{1}{1-\rho^2}\left[\left(\frac{y - \mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right) - \left(\frac{\rho\left(\ln\gamma_D - \mu_{\gamma_D}\right)}{\sqrt{2}\sigma_{\gamma_D}}\right)\right]^2\right\} dy d\gamma_D$$

$$= \int_0^{\infty} \ln\left(1+\gamma_D\right) \Phi\left(\frac{\ln\gamma_D - \mu_{\gamma_E} - \rho\frac{\sigma_{\gamma_E}}{\sigma_{\gamma_D}}\left(\ln\gamma_D - \mu_{\gamma_D}\right)}{\sqrt{\left(1-\rho^2\right)}\sigma_{\gamma_E}}\right) \frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}\gamma_D} \exp\left\{-\left(\frac{\ln\gamma_D - \mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)^2\right\} d\gamma_D \tag{14}$$

Similarly, we have

$$D_2 = \int_0^{\infty} \ln\left(1+\gamma_E\right) Q\left(\frac{\ln\gamma_E - \mu_{\gamma_D} - \rho\frac{\sigma_{\gamma_D}}{\sigma_{\gamma_E}}\left(\ln\gamma_E - \mu_{\gamma_E}\right)}{\sqrt{\left(1-\rho^2\right)}\sigma_{\gamma_D}}\right) \frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}\gamma_E} \exp\left\{-\left(\frac{\ln\gamma_E - \mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right)^2\right\} d\gamma_E \tag{15}$$

Similarly to the derivation of $\bar{C}_D'\left(\gamma_D\right)$ in the above subsection, we can have

$$D_1 \approx \frac{2}{3}\psi_{D_1}\left(\mu_{\gamma_D}\right) + \frac{1}{6}\psi_{D_1}\left(\mu_{\gamma_D} + \sqrt{3}\sigma_{\gamma_D}\right) + \frac{1}{6}\psi_{D_1}\left(\mu_{\gamma_D} - \sqrt{3}\sigma_{\gamma_D}\right) \tag{16-a}$$

$$D_2 \approx \frac{2}{3}\psi_{D_2}\left(\mu_{\gamma_E}\right) + \frac{1}{6}\psi_{D_2}\left(\mu_{\gamma_E} + \sqrt{3}\sigma_{\gamma_E}\right) + \frac{1}{6}\psi_{D_2}\left(\mu_{\gamma_E} - \sqrt{3}\sigma_{\gamma_E}\right) \tag{16-b}$$

where $\psi_{D_1}\left(x\right) = \ln\left(1+\exp\left(x\right)\right)\Phi\left(\frac{x - \mu_{\gamma_E} - \rho\frac{\sigma_{\gamma_E}}{\sigma_{\gamma_D}}\left(\ln x - \mu_{\gamma_D}\right)}{\sqrt{\left(1-\rho^2\right)}\sigma_{\gamma_E}}\right)$ and

$$\psi_{D_2}\left(x\right) = \ln\left(1+\exp\left(x\right)\right) Q\left(\frac{x - \mu_{\gamma_D} - \rho\frac{\sigma_{\gamma_D}}{\sigma_{\gamma_E}}\left(\ln x - \mu_{\gamma_E}\right)}{\sqrt{\left(1-\rho^2\right)}\sigma_{\gamma_D}}\right).$$

3.3 Independent composite fading channels

While the receiver is subject to the composite multipath/shadowed signal, wireless channels are commonly modeled as a mixture of multipath fading and shadowing, which is a general case for communication systems with low mobility or stationary users [34, 35]. This model is also encountered in certain land-mobile satellite systems (see [36] and the references therein).

Assume the main and eavesdropper channels experience independent fading, and the Generalized-*K* channel models are adopted to study the secrecy capacity in composite fading environments. As suggested by [37], we have the pdf of the output SNR as

$$p(\gamma_i) = \frac{\alpha^{\beta+1}}{2^{\beta}\Gamma(n_i)\Gamma(m_i)} \gamma_i^{\frac{\beta-1}{2}} K_{\alpha}\left(a\sqrt{\gamma_i}\right), \quad i \in \{D, E\} \qquad (17)$$

Where m_i and n_i are the shaping parameters of the distribution of *i* channel, with $\alpha = m_i - n_i$ and $\beta = m_i + n_i - 1$, and $K_{\alpha}(\cdot)$ is the modified Bessel function of order α [41, Eq.(8.407/1)]. In Eq.(17), $a = \sqrt{\frac{4l_i n_i}{\overline{\gamma_i}}}$ where $\overline{\gamma_i}$ is the average SNR. In general, the parameter *m* is a positive real number. In our analysis, assume that *m* is an integer, and no condition is imposed on *k* so it can take arbitrary positive real values. An important special case falls under the assumption that *m* = 1, which corresponds to the *K*-distribution.

For arbitrary α and β, the ergodic capacity of Generalized-*K* channels was studied and presented in terms of Meijer-*G* functions in [38]. Since the evaluation of Meijer-*G* functions can be sometimes laborious, our work proposes an alternative approach to derive the closed-form expressions of the average secrecy capacity over Generalized-*K* channels.

Denoting $\gamma_i \square G(k_i, \theta_i)$ ($i \in \{D, E\}$) as a Gamma distributed random variable with a shape parameter k_i and a scale parameter θ_i, the pdf of γ_i is given as

$$p(\gamma_i; \theta_i, k_i) = \frac{\theta_i^{-k_i}}{\Gamma(k_i)} \gamma_i^{k_i - 1} \exp\left(-\frac{\gamma_i}{\theta_i}\right), \quad i \in \{D, E\} \qquad (18)$$

where $\Gamma(x) = \int_0^{\infty} t^{x-1} \exp(-t) dt \quad \text{for } x > 0$.

As indicated in [39], when applying the first and second moment matching to approximate the generalized-*K* distribution by a Gamma distribution, the shapeand scale parameters in Eq. (18) can be rewritten as

$$\theta_i = [AF - \varepsilon]\Omega_i, \; 0 \le AF \le AF_{\max}, \; \varepsilon_0 \le \varepsilon \le AF \qquad (19\text{-a})$$

$$k_i = \frac{1}{AF - \varepsilon}, \; 0 \le AF \le AF_{\max}, \; \varepsilon_0 \le \varepsilon \le AF \qquad (19\text{-b})$$

where *AF* is the amount of fading and $AF = \frac{1}{m_i} + \frac{1}{n_i} + \frac{1}{m_i n_i}$, $AF_{\max}$ is finite and the upper bound of *AF*. Ω_i is the mean of the received local power over *i* channel, and ε is the adjustment factor. In practical the relevant range of ε is $[-8, 8]$, and $\varepsilon_0 \ge -AF$. Furthermore, ε can be computed using a numerical measure of the difference between the approximated and the approximating pdf

(cdf) [39].

Therefore, the average secrecy capacity over Generalized-*K* channels can be written as

$$\begin{aligned}\bar{C}_s(\gamma_D,\gamma_E) &= \int_0^\infty \ln(1+\gamma_D)\, p(\gamma_D;\theta_D,k_D)\int_0^{\gamma_D} p(\gamma_E;\theta_E,k_E)d\gamma_E d\gamma_D \\ &\quad - \int_0^\infty \ln(1+\gamma_E)\, p(\gamma_E;\theta_E,k_E)\int_{\gamma_E}^\infty p(\gamma_D;\theta_D,k_D)d\gamma_D d\gamma_E \\ &= \int_0^\infty \ln(1+\gamma_D)\, p(\gamma_D;\theta_D,k_D)\int_0^{\gamma_D} p(\gamma_E;\theta_E,k_E)d\gamma_E d\gamma_D \\ &\quad + \int_0^\infty \ln(1+\gamma_E)\, p(\gamma_E;\theta_E,k_E)\int_0^{\gamma_E} p(\gamma_D;\theta_D,k_D)d\gamma_D d\gamma_E \\ &\quad - \int_0^\infty \ln(1+\gamma_E)\, p(\gamma_E;\theta_E,k_E)d\gamma_E \\ &= E_1 + E_2 - E_3\end{aligned} \tag{20}$$

where $E_1 = \dfrac{1}{\Gamma(k_E)}\int_0^\infty \ln(1+\gamma_D)\, p(\gamma_D;\theta_D,k_D)\phi\left(k_E,\dfrac{\gamma_D}{\theta_E}\right)d\gamma_D$,

$E_2 = \dfrac{1}{\Gamma(k_D)}\int_0^\infty \ln(1+\gamma_E)\, p(\gamma_E;\theta_E,k_E)\phi\left(k_D,\dfrac{\gamma_E}{\theta_D}\right)d\gamma_E$,

$E_3 = \int_0^\infty \ln(1+\gamma_E)\, p(\gamma_E;\theta_E,k_E)d\gamma_E$,and $\phi(s,x)$ is the lower incomplete gamma function and $\phi(s,x) = \int_0^x t^{s-1}\exp(-t)dt$.

A gamma approximation of log-normal distribution pdf was proposed in [40]. Herein, we reverse using this approach to obtain E_1 and E_2. Eq. (18) can be approximated by the following log-normal distribution

$$f(\gamma_i;\mu_i,\sigma_i) = \frac{1}{\gamma_i\sqrt{2\pi\sigma_i^2}}\exp\left(-\frac{(\ln\gamma_i-\mu_i)^2}{2\sigma_i^2}\right), \quad i\in\{D,E\} \tag{21}$$

where μ_i and σ_i are the mean and variance for γ_i's natural logarithm, respectively, which can be written as

$$\mu_{\gamma_i}' = \ln\frac{\theta_i}{\sqrt{k_i^2+k_i}} \tag{22-a}$$

$$\sigma_{\gamma_i}' = \sqrt{\ln\left(1+k_i^{-1}\right)}\,. \tag{22-b}$$

Then substituting Eq. (21) into E_1, we obtain

$$E_1 \approx \frac{1}{\Gamma(k_E)}\int_0^\infty \Delta_D(\gamma_D)\frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}'\gamma_D}\exp\left[-\left(\frac{\ln\gamma_D-\mu_{\gamma_D}'}{\sqrt{2}\sigma_{\gamma_D}'}\right)^2\right]d\gamma_D \tag{23}$$

where $\Delta_D(\gamma_D) = \ln(1+\gamma_D)\phi\left(k_E,\dfrac{\gamma_D}{\theta_E}\right)$.

By using Eq. (8), we finally obtain

$$E_1 \approx \frac{1}{6\Gamma(k_E)}\left[4\Delta_D(\mu_{\gamma_D}') + \Delta_D\left(\mu_{\gamma_D}'+\sqrt{3}\sigma_{\gamma_D}'\right) + \Delta_D\left(\mu_{\gamma_D}'-\sqrt{3}\sigma_{\gamma_D}'\right)\right] \tag{24}$$

Similarly, we obtain

$$E_2 \approx \frac{1}{6\Gamma(k_D)}\left[4\Delta_E\left(\mu_{\gamma_E}'\right)+\Delta_E\left(\mu_{\gamma_E}'+\sqrt{3}\sigma_{\gamma_E}'\right)+\Delta_E\left(\mu_{\gamma_E}'-\sqrt{3}\sigma_{\gamma_E}'\right)\right] \quad (25)$$

where $\Delta_E\left(\gamma_E\right)=\ln\left(1+\gamma_E\right)\phi\left(k_D,\frac{\gamma_E}{\theta_D}\right)$.

By using Eqs. 9.121.6and 7.522.5 in [41], we obtain one expression of E_3, i.e.,

$$E_3 = k_E\theta_E\,{}_3F_1\left(k_E+1,1,1;2;-\theta_E\right),\ \theta_E>0 \quad (26)$$

where ${}_qF_p$ is the generalized hypergeometric series (Eq. 9.14.1) in [41].

Then, the average secrecy capacity over Generalized-*K* channels can also be obtained by substituting Eqs. (24), (25) and (26) into Eq. (20).

4. Secrecy outage analysis over non-small scale fading channels

In this section, we carry out the analysis on secrecy outage performance over three different types of non-small scale fading channels: independent/ correlated log-normal fading channels, and independent composite fading channel.

4.1 Independent log-normal fading

As the main and eavesdropper channels experience independent log-normal fading, the probability of non-zero secrecy capacity is given by

$$\begin{aligned}\Pr\left\{C_s\left(\gamma_D,\gamma_E\right)>0\right\} &= \Pr\left\{\ln\left(1+\gamma_D\right)>\ln\left(1+\gamma_E\right)\right\}=\Pr\left\{\gamma_D>\gamma_E\right\}\\ &= \int_0^\infty\int_0^{\gamma_D} f\left(\gamma_D;\mu_{\gamma_D},\sigma_{\gamma_D}\right)f\left(\gamma_E;\mu_{\gamma_E},\sigma_{\gamma_E}\right)d\gamma_E d\gamma_D\\ &= \int_0^\infty f\left(\gamma_D;\mu_{\gamma_D},\sigma_{\gamma_D}\right)\Phi\left(\frac{\ln\gamma_D-\mu_{\gamma_E}}{\sigma_{\gamma_E}}\right)d\gamma_D\\ &= \int_0^\infty f\left(\gamma_D;\mu_{\gamma_D},\sigma_{\gamma_D}\right)\left[1-Q\left(\frac{\ln\gamma_D-\mu_{\gamma_E}}{\sigma_{\gamma_E}}\right)\right]d\gamma_D\\ &= 1-\int_0^\infty f\left(\gamma_D;\mu_{\gamma_D},\sigma_{\gamma_D}\right)Q\left(\frac{\ln\gamma_D-\mu_{\gamma_E}}{\sigma_{\gamma_E}}\right)d\gamma_D\end{aligned} \quad (27)$$

where $Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt$ is the Gaussian Q-function.

By using Eq. (8), we have

$$\Pr\left\{C_s\left(\gamma_D,\gamma_E\right)>0\right\}\approx 1-\frac{2}{3}Q\left(\frac{\mu_{\gamma_D}-\mu_{\gamma_E}}{\sigma_{\gamma_E}}\right)-\frac{1}{6}Q\left(\frac{\mu_{\gamma_D}+\sqrt{3}\sigma_{\gamma_D}-\mu_{\gamma_E}}{\sigma_{\gamma_E}}\right)-\frac{1}{6}Q\left(\frac{\mu_{\gamma_D}-\sqrt{3}\sigma_{\gamma_D}-\mu_{\gamma_E}}{\sigma_{\gamma_E}}\right) \quad (28)$$

In this work, we define the secure outage probability as

$$
\begin{aligned}
\Pr_{out}\left(C_{th}\right) &= \Pr\left\{C_s\left(\gamma_D,\gamma_E\right) < C_{th}\right\} \\
&= \Pr\left\{\ln\left(1+\gamma_D\right) - \ln\left(1+\gamma_E\right) < C_{th}\right\} \\
&= \Pr\left\{\ln\left(1+\gamma_D\right) - \ln\left(1+\gamma_E\right) < \ln\left(\exp\left(C_{th}\right)\right)\right\} \\
&= \Pr\left\{\ln\frac{1+\gamma_D}{1+\gamma_E} < \ln\left(\exp\left(C_{th}\right)\right)\right\} \\
&= \Pr\left\{\frac{1+\gamma_D}{1+\gamma_E} < \exp\left(C_{th}\right)\right\} \\
&= \Pr\left\{\gamma_D < \exp\left(C_{th}\right)\cdot\gamma_E + \exp\left(C_{th}\right) - 1\right\} \\
&= \Pr\left\{\gamma_D < \lambda\gamma_E + \lambda - 1\right\}
\end{aligned}
\tag{29}
$$

where C_{th} ($C_{th} > 0$) is the target secrecy capacity threshold, and $\lambda = \exp\left(C_{th}\right)$.

As the main and eavesdropper channels experience independent log-normal fading, the secure outage probability $\Pr_{out}\left(C_{th}\right)$ is given by

$$
\begin{aligned}
\Pr_{out}\left(C_{th}\right) &= \Pr\left\{\gamma_D < \lambda\gamma_E + \lambda - 1\right\} \\
&= \int_0^{\infty} f\left(\gamma_E;\mu_{\gamma_E},\sigma_{\gamma_E}\right)\int_0^{\lambda\gamma_E+\lambda-1} f\left(\gamma_D;\mu_{\gamma_D},\sigma_{\gamma_D}\right)d\gamma_D d\gamma_E \\
&= \int_0^{\infty} f\left(\gamma_E;\mu_{\gamma_E},\sigma_{\gamma_E}\right)\Phi\left(\frac{\ln\left(\lambda\gamma_E+\lambda-1\right)-\mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)d\gamma_E \\
&= \int_0^{\infty} f\left(\gamma_E;\mu_{\gamma_E},\sigma_{\gamma_E}\right)\left[1-Q\left(\frac{\ln\left(\lambda\gamma_E+\lambda-1\right)-\mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)\right]d\gamma_E \\
&= 1-\int_0^{\infty} f\left(\gamma_E;\mu_{\gamma_E},\sigma_{\gamma_E}\right)Q\left(\frac{\ln\left(\lambda\gamma_E+\lambda-1\right)-\mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)d\gamma_E
\end{aligned}
\tag{30}
$$

By using Eq. (8), we have

$$
\Pr_{out}\left(C_{th}\right) \approx 1-\frac{2}{3}Q\left(\frac{\varphi\left(\mu_{\gamma_E}\right)-\mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)-\frac{1}{6}Q\left(\frac{\varphi\left(\mu_{\gamma_E}+\sqrt{3}\sigma_{\gamma_E}\right)-\mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)-\frac{1}{6}Q\left(\frac{\varphi\left(\mu_{\gamma_E}-\sqrt{3}\sigma_{\gamma_E}\right)-\mu_{\gamma_D}}{\sigma_{\gamma_D}}\right)
\tag{31}
$$

where $\varphi(x) = \ln\left(\lambda\exp(x)+\lambda-1\right)$.

4.2 Correlated log-normal fading

As the main and eavesdropper channels experience correlated log-normal fading, similarly to the above subsection, the probability of non-zero secrecy capacity can be given by

$$\begin{aligned}\Pr\left\{C_s\left(\gamma_D,\gamma_E\right)>0\right\} &= \Pr\left\{\gamma_D>\gamma_E\right\}\\ &= \int_0^{\infty}\int_0^{\gamma_D} p_{\gamma_D,\gamma_E}\left(\gamma_D,\gamma_E\right)d\gamma_E d\gamma_D\\ &= \frac{1}{\sqrt{1-\rho^2}}\int_0^{\infty}\frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}\gamma_D}\exp\left[-\frac{1}{1-\rho^2}\cdot\frac{\left(\ln\gamma_D-\mu_{\gamma_D}\right)^2}{2\sigma_{\gamma_D}^2}\right]\\ &\int_0^{\gamma_D}\frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}\gamma_E}\cdot\exp\left\{-\frac{1}{1-\rho^2}\left[\frac{\left(\ln\gamma_E-\mu_{\gamma_E}\right)^2}{2\sigma_{\gamma_E}^2}-2\rho\left(\frac{\ln\gamma_D-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)\left(\frac{\ln\gamma_E-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right)\right]\right\}d\gamma_E d\gamma_D\end{aligned} \quad (32)$$

Let $a=\frac{1}{\sqrt{1-\rho^2}}$, $x_1=\frac{\ln\gamma_D-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}$ and $x_2=\frac{\ln\gamma_E-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}$, then we have $\frac{\ln\gamma_D-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}=kx_1+b$,

where $k=\frac{\sigma_{\gamma_D}}{\sigma_{\gamma_E}}$ and $b=\frac{\mu_{\gamma_D}-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}$. Thus, we can rewrite Eq. (32) as

$$\begin{aligned}\Pr\left\{C_s\left(\gamma_D,\gamma_E\right)>0\right\} &= \frac{a}{\pi}\int_{-\infty}^{\infty}\exp\left(-a^2x_1^2\right)\int_{-\infty}^{kx_1+b}\exp\left(-a^2\left(x_2^2-2\rho x_1x_2\right)\right)dx_2dx_1\\ &= \frac{a}{\pi}\int_{-\infty}^{\infty}\exp\left(-a^2x_1^2\right)\cdot\frac{\sqrt{\pi}}{2a}\exp\left(\rho^2a^2x_1^2\right)erf\left(ax_2-\rho ax_1\right)\Big|_{x_2=-\infty}^{x_2=kx_1+b}dx_1\\ &= \frac{1}{2\sqrt{\pi}}\int_{-\infty}^{\infty}\exp\left(-x_1^2\right)\cdot\left[erf\left(a\left(k-\rho\right)x_1+ab\right)+1\right]dx_1\end{aligned} \quad (33)$$

where $erf\left(x\right)$ is the error function, which is defined as $erf\left(x\right)=\frac{2}{\sqrt{\pi}}\int_0^x\exp\left(-t^2\right)dt$.

It is obvious that $\sqrt{2}x_1 \sim N\left(0,2\right)$. Then, by using Eq. (8), we obtain

$$\begin{aligned}&\Pr\left\{C_s\left(\gamma_D,\gamma_E\right)>0\right\}\\ &\approx\frac{1}{6\sqrt{2}}\left\{4\left[erf\left(ab\right)+1\right]+\left[erf\left(\sqrt{6}a\left(k-\rho\right)+ab\right)+1\right]+\left[erf\left(ab-\sqrt{6}a\left(k-\rho\right)\right)+1\right]\right\}\\ &=\frac{1}{6\sqrt{2}}\left\{4erf\left(ab\right)+erf\left(\sqrt{6}a\left(k-\rho\right)+ab\right)+erf\left(ab-\sqrt{6}a\left(k-\rho\right)\right)+6\right\}\end{aligned} \quad (34)$$

Similarly to the above subsection, we can present the secure outage probability $\Pr_{out}\left(C_{th}\right)$ over correlated log-normal fading channels as

$$\begin{aligned}\Pr_{out}\left(C_{th}\right) &= \Pr\left\{\gamma_D<\lambda\gamma_E+\lambda-1\right\}\\ &= \int_0^{\infty}\int_0^{\lambda\gamma_E+\lambda-1} p_{\gamma_D,\gamma_E}\left(\gamma_D,\gamma_E\right)d\gamma_D d\gamma_E\\ &= \frac{1}{\sqrt{1-\rho^2}}\int_0^{\infty}\frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}\gamma_E}\exp\left[-\frac{1}{1-\rho^2}\cdot\frac{\left(\ln\gamma_E-\mu_{\gamma_E}\right)^2}{2\sigma_{\gamma_E}^2}\right]\\ &\int_0^{\lambda\gamma_E+\lambda-1}\frac{1}{\sqrt{2\pi}\sigma_{\gamma_D}\gamma_D}\cdot\exp\left\{-\frac{1}{1-\rho^2}\left[\frac{\left(\ln\gamma_D-\mu_{\gamma_D}\right)^2}{2\sigma_{\gamma_D}^2}-2\rho\left(\frac{\ln\gamma_E-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right)\left(\frac{\ln\gamma_D-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}\right)\right]\right\}d\gamma_D d\gamma_E\end{aligned} \quad (35)$$

where C_{th} ($C_{th}>0$) is the target secrecy capacity threshold, and $\lambda=\exp\left(C_{th}\right)$.

Let $y=\dfrac{\ln\gamma_D-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}$, then we can rewrite Eq. (35) as

$$\begin{aligned}\Pr_{out}\left(C_{th}\right)&=\frac{1}{\sqrt{1-\rho^2}}\int_0^{\infty}\frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}\gamma_E}\exp\left[-\frac{1}{1-\rho^2}\cdot\frac{(\ln\gamma_E-\mu_{\gamma_E})^2}{2\sigma_{\gamma_E}^2}\right]\\&\quad\int_{-\infty}^{\varphi(\gamma_E)}\frac{1}{\sqrt{\pi}}\cdot\exp\left\{-\frac{1}{1-\rho^2}\left[y^2-2\rho y\left(\frac{\ln\gamma_E-\mu_{\gamma_E}}{\sqrt{2}\sigma_{\gamma_E}}\right)\right]\right\}dyd\gamma_E\\&=\frac{1}{\sqrt{1-\rho^2}}\int_0^{\infty}\frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}\gamma_E}\exp\left[-\frac{(\ln\gamma_E-\mu_{\gamma_E})^2}{2\sigma_{\gamma_E}^2}\right]\cdot g\left(\gamma_E\right)d\gamma_E\end{aligned}\tag{36}$$

where $g\left(\gamma_E\right)=\dfrac{\sqrt{1-\rho^2}}{2}\left[1+erf\left(\dfrac{\varphi\left(\gamma_E\right)-\rho\dfrac{\ln\gamma_E-\mu_E}{\sqrt{2}\sigma_{\gamma_E}}}{\sqrt{1-\rho^2}}\right)\right]$ and

$\varphi\left(\gamma_E\right)=\dfrac{\ln\left(\lambda\gamma_E+\lambda-1\right)-\mu_{\gamma_D}}{\sqrt{2}\sigma_{\gamma_D}}$.

By using Eq. (8), we can have

$$\Pr_{out}\left(C_{th}\right)\approx\frac{1}{6}\left[4g\left(\mu_{\gamma_E}\right)+g\left(\mu_{\gamma_E}+\sqrt{3}\sigma_{\gamma_E}\right)+g\left(\mu_{\gamma_E}-\sqrt{3}\sigma_{\gamma_E}\right)\right]\tag{37}$$

4.3 Independent composite fading channels

Assume that the main and eavesdropper channels experience independent composite fading, similarly to the above subsection 4.1 and by using Eq. (17), the probability of non-zero secrecy capacity can beapproximated as

$$\begin{aligned}\Pr\left\{C_s\left(\gamma_D,\gamma_E\right)>0\right\}&=\Pr\left\{\gamma_D>\gamma_E\right\}\\&\approx\int_0^{\infty}p\left(\gamma_D;\theta_D,k_D\right)\int_0^{\gamma_D}p\left(\gamma_E;\theta_E,k_E\right)d\gamma_Ed\gamma_D\\&=\frac{1}{\Gamma\left(k_E\right)}\int_0^{\infty}p\left(\gamma_D;\theta_D,k_D\right)\phi\left(k_E,\frac{\gamma_D}{\theta_E}\right)d\gamma_D\end{aligned}\tag{38}$$

By using Eq. (6.455-2) in [41], we obtain the probability of non-zero secrecy capacity as

$$\Pr\left\{C_s\left(\gamma_D,\gamma_E\right)>0\right\}\approx\frac{\theta_D^{-k_D}\theta_E^{-k_E}}{k_E\left(\theta_E^{-1}+\theta_E^{-1}\right)^{k_D+k_E}}\cdot\frac{\Gamma\left(k_D+k_E\right)}{\Gamma\left(k_D\right)\Gamma\left(k_E\right)}\cdot{}_2F_1\left(1,k_D+k_E;k_E+1;\frac{\theta_D}{\theta_D+\theta_E}\right)\tag{39}$$

Similarly to subsection 4.2, we present the secure outage probability $\Pr_{out}\left(C_{th}\right)$ over independent composite fading channels as

$$\begin{aligned}\Pr_{out}\left(C_{th}\right)&=\Pr\left\{\gamma_D<\lambda\gamma_E+\lambda-1\right\}\\&=\int_0^{\infty}p\left(\gamma_E;\theta_E,k_E\right)\int_0^{\lambda\gamma_E+\lambda-1}p\left(\gamma_D;\theta_D,k_D\right)d\gamma_Dd\gamma_E\\&=\frac{1}{\Gamma\left(k_D\right)}\int_0^{\infty}p\left(\gamma_E;\theta_E,k_E\right)\phi\left(k_D,\frac{\lambda\gamma_E+\lambda-1}{\theta_D}\right)d\gamma_E\end{aligned}\tag{40}$$

To obtain a closed-form expression for Eq. (40), we reverse what we have done in Section 3.3, that is, by adopting a log-normal approximation of gamma pdf, then we have

$$\Pr_{out}\left(C_{th}\right) \approx \frac{1}{\Gamma\left(k_D\right)} \int_0^{\infty} \phi\left(k_D, \frac{\lambda\gamma_E + \lambda - 1}{\theta_D}\right) \frac{1}{\sqrt{2\pi}\sigma_{\gamma_E}'\gamma_E} \exp\left[-\left(\frac{\ln\gamma_E - \mu_{\gamma_E}'}{\sqrt{2}\sigma_{\gamma_E}'}\right)^2\right] d\gamma_E \quad (41)$$

By using Eq. (8), we finally obtain the approximation for the secure outage probabilityover independent composite fading channels as

$$\Pr_{out}\left(C_{th}\right) \approx$$

$$\frac{1}{6\Gamma\left(k_D\right)}\left[4\phi\left(k_D, \frac{\lambda\mu_{\gamma_E}' + \lambda - 1}{\theta_D}\right) + \phi\left(k_D, \frac{\lambda\left(\mu_{\gamma_E}' + \sqrt{3}\sigma_{\gamma_E}'\right) + \lambda - 1}{\theta_D}\right) + \phi\left(k_D, \frac{\lambda\left(\mu_{\gamma_E}' - \sqrt{3}\sigma_{\gamma_E}'\right) + \lambda - 1}{\theta_D}\right)\right] \quad (42)$$

5. Numerical results and discussion

Here, we compare simulation and analysis results for the secrecy capacity and secrecy outage (including PNSC and SOP) over independent/correlated lognormal shadowing channels and composite fading channels. The parameters are set to Pt =1, $\omega D = \omega E = 1$, $\sigma D = \sigma E = 1$, and Cth = 0 dB. Simulation is performed by transmitting 1×10^6 bits. The unit for the average secrecy capacity is bits/channel use.

A. Numerical results

In Figs. 2 and 3, we compare simulation and analysis results of the average secrecy capacity over independent/correlated lognormal shadowing channels. One can see that our analysis results match the simulation results very well. This shows the accuracy of the approximation. It can be observed that the average secrecy capacity over independent lognormal fading channel for a higher $\mu\gamma E$ outperforms that for a lower $\mu\gamma E$. A higher $\mu\gamma E$ represents a better secure channel condition for the *S*–*D* communication pair, because the channel capacity difference between the main and eavesdropper channels increases with $\mu\gamma E$ for a given $\mu\gamma D/\mu\gamma E$. Moreover, we also note that the average secrecy capacity over a correlated lognormal fading channel for a lower ρ outperforms that for a higher ρ due to a higher ρ representing a stronger correlation between the main and eavesdropper channels.

Similar observations can be also made from Figs. 4–7 for the PNSC and SOP over independent/correlated lognormal fading channels. More specifically, we can observe that ρ has an opposite influence on the PNSC and SOP over a correlated lognormal fading channel on both sides of the cutoff (−0.5 and 0.5 dB in Figs. 6 and 7, respectively). As shown in Figs. 4 and 5, the PNSC over independent/correlated lognormal fading channels has a cutoff (0 dB). Furthermore, as shown in Figs. 6 and 7, the SOP over independent and correlated lognormal fading channels has a cutoff of −0.3 and 0.7 dB, respectively.

On the other hand, in Figs. 4 and 5, we can find that simulation and analysis results do not match well for PNSC in low $\mu\gamma D/\mu\gamma E$ for lower $\mu\gamma E$. This difference mainly arises from the approximation method adopted to deal with the integral of the function of lognormal variables in (4).

As shown in Fig. 5, we can also see that the PNSC with a higher ρ outperforms that with a lower ρ while $\mu_{\gamma D}/\mu_{\gamma E}$ is positive. A similar conclusion can be made for the SOP when $\mu_{\gamma D}/\mu_{\gamma E}$ is larger than 0.7 dB, as shown in Fig. 7.

Moreover, we can also observe that all PNSC curves converge to the same horizontal asymptote (SOP = 1) while $\mu_{\gamma D}/\mu_{\gamma E}$ increases. As presented in Figs. 6 and 7, it is obvious that all SOP curves go very smoothly when $\mu_{\gamma D}/\mu_{\gamma E}$ is not larger than −0.3 and 0.7 dB, respectively.

In Figs. 8–10, we present the results for composite fading channels. It can be observed that analysis results match the simulation results very well. A higher $\mu_{\gamma E}$ outperforms a lower $\mu_{\gamma E}$. A higher $\mu_{\gamma E}$ represents a better secure channel condition for the main link (*S*–*D*), since the channel capacity difference between the main and eavesdropper channels increases with $\mu_{\gamma E}$ given a fixed $\mu_{\gamma D}/\mu_{\gamma E}$.Moreover, there is a cutoff of −1.2, 0, and −1 dB, in Figs. 8–10, respectively.

Figs. 11–13 present simulation results to compare the average secrecy capacity, PNSC, and SOP over independent/correlated lognormal and composite fading channels, when ρ = 0.4 and $\mu_{\gamma E}$ = 2 and 5. In these figures, we can see that average secrecy capacity, PNSC, and SOP have a cutoff of 0 dB.

In Fig. 11, it is obvious that the average secrecy capacity over composite fading channels outperforms those over the two other fading channels when $\mu_{\gamma D}/\mu_{\gamma E}$ is negative. The average secrecy capacities over the three considered fading channels are similar when $\mu_{\gamma D}/\mu_{\gamma E}$ is positive.

In Fig. 12, we can observe that the PNSC over composite fading channels outperforms those over the two other fading channels when $\mu_{\gamma D}/\mu_{\gamma E}$ is negative, and the PNSC over correlated lognormal fading channels outperforms those over the other two fading channels when $\mu_{\gamma D}/\mu_{\gamma E}$ is positive.

In Fig. 13, the SOP over correlated lognormal fading channels outperforms those over the other two fading channels when $\mu_{\gamma D}/\mu_{\gamma E}$ is positive.

B. Computation Time and Accuracy Analysis

In the following, the computation time and the accuracy analysis of our proposed analytical expressions are discussed for the considered system over independent/correlated lognormal fading channels and composite fading channels.

As observed from Table I, benefiting from the adopted approximations, our analytical expressions save much time compared with simulations. Thus, we can conclude that our proposed analytical models are suitable for practical application due to its low computational complexity.

To facilitate the accuracy analysis, in the following, we denote $\theta = \mu_{\gamma D}/\mu_{\gamma E}$. We present a useful measure to illustrate the accuracy of our proposed analytical models as

$$\text{error} = (\text{simulation results} - \text{analytical results}) / \text{simulation results} \times 100\%.$$

As shown in Tables II–X, we can see that the discrepancies between the analytical and simulation results are quite small in most cases. In Tables II and V, the computational errors in Figs. 2 and 5 are large, as mentioned earlier, but within ±35% in the low-$\mu_{\gamma D}/\mu_{\gamma E}$ region. However, low $\mu_{\gamma D}/\mu_{\gamma E}$ represents the cases when the *S*–*D* link is much worse than the *S*–*E* link (that is to say, *E* locates very close to *S*), which are quite rare in practical scenarios.

Thus, we can conclude that our proposed analytical models can work well in most practical cases with low computational complexity and error.

6. Conclusion

In this paper, we have investigated the average secrecy capacity and secrecy outage (including PNSC and SOP) of secure communications over independent/correlated lognormal fading channels and composite fading channels. The approximate closed-form expressions for these performance indexes have been derived, whose accuracies have been verified by simulation results.

The parameters chosen in Section 5 are from practical scenarios [41], [42]. Thus, our results are at least useful for these applications, although the accuracy may decrease for other applications. There are considerable errors between simulation and analysis results in Figs. 2 and 5, but they only occur in the lower $\mu\gamma D/\mu\gamma E$ region, when the *S*–*D* link is much worse than the *S*–*E* link (that is, *E* locates very close to *S* and is rare in practical applications). Moreover, most of the errors are on the order of 10^{-3} or 10^{-4}, which are acceptable in practical applications.

7. Reference

[1] B. Schneier, "Cryptographic design vulnerabilities," *Comput.*, vol. 31, no. 9, pp. 29-33, Sep. 1998.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no.8, pp. 1355-1367, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, Jul.1978.

[5] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005, pp. 2152-2155.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 356-360.

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[8] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp.4687-4698, Oct. 2008.

[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[10] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453-2469, Jun. 2008.

[11] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no.6, pp. 2547-2553, Jun. 2009.

[12] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wiretap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033-4039, Sept. 2009.

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part I: the MISOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: the MIMOME wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[15] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp.

4961-4972, Aug. 2011.

[16] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2673-2682, May 2013.

[17] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collin, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commu.*, vol. 61, no. 1, pp. 144-154, Jan. 2013.

[18] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 4005-4019, Apr. 2011.

[19] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Sig. Process. Lett.*, vol. 19, no. 8, pp. 479-482, Aug. 2012.

[20] Matthias Pätzold, Mobile Radio Channels, 2nd Edition. New York: John Wiley & Sons, Inc., 2012.

[21] Christopher Haslett, Essentials of radio wave propagation, Cambridge UK: Cambridge University Press, 2008.

[22] F. Molisch, J. R. Foerster and M. Pendergrass, "Channel models for ultrawideband personal area networks," *IEEE Wireless Commun.*, vol.10, no. 6, pp. 14-21, Dec. 2003.

[23] X. Liu, "Secrecy capacity of wireless links subject to log-normal fading," in *Proc. 2012 7th International ICST Conference on Communications and Networking in China (CHINACOM)*, Kunming, China, Aug. 8-10 2012, pp. 167-172.

[24] Md. Zahurul I. Sarkar, T. Ratnarajah, "Secrecy capacity over correlated log-normal fading channel," in *Proc. ICC 2012*, Ottawa, Canada, June 10-15 2012, pp. 883-887.

[25] A. Laourine, A. Stephenne, and S. Affes, "Estimating the ergodic capacity of log-normal channels," *IEEE Commun. Lett.*, vol. 11, no. 7, pp. 568-570, Jul. 2007.

[26] F. Hédiot, X. Chu, R. Hoshyar, and A. Tafazolli, "A tight closed-form approximation of the log-normal fading channel capacity," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2842-2847, Jun. 2009.

[27] G. Pan, E. Eylem and Q. Feng, "Capacity analysis of log-normal channel under various adaptive transmission schemes," *IEEE Commu. Lett.*, vol. 16, no. 3, pp. 346-348, Mar. 2012.

[28] G. Pan, E. Eylem and Q. Feng, "Performance analysis of cooperative time hopping UWB systems with multi-user interference," *IEEE Trans. Wireless Commu.*, vol. 11, no. 6, pp. 1969-1975, Jun. 2012.

[29] J. M.Holtzman, "A simple, accurate method to calculate spread multiple-access error probabilities," *IEEE Trans.Commu.*, vol. 40, no. 3, pp. 461-464, Mar. 1992.

[30] D. Skraparlis, V. K. Sakarellos, A. D. Panagopoulos, J. D. Kanellopoulos, "Performance of *N*-branch receive diversity combining in correlated lognormal channels," *IEEE Commun. Lett.*, vol. 13, no. 7, pp. 489-491, Jul.2009.

[31] D. Skraparlis, V. K. Sakarellos, A. D. Panagopoulos, J. D. Kanellopoulos, "New results on the statistics and the capacity of dual-branch MRC and EGC diversity in correlated lognormal channels," *IEEE Commun. Lett.*, vol. 15, no. 6, pp. 617-619, Jun.2011.

[32] D. Skraparlis, M. Sandell, V. K. Sakarellos, A. D. Panagopoulos, J. D. Kanellopoulos, "On the effect of correlation on the performance of dual diversity receivers in lognormal fading," *IEEE Commun. Lett.*, vol. 14, no. 11, pp. 1038-1040, Nov. 2010.

[33] M. Alouini and M. Simon, "Dual diversity over correlated log-normal fading channels," *IEEE Trans. Commun.*, vol. 50, no. 12, pp. 1946-1959, Dec.2002.

[34] M. J. Ho and G. L. Stüber, "Co-channel interference of microcellular systems on shadowed Nakagami fading channels," in *Proc. IEEE Veh. Technol. Conf. (VTC'93)*, 1993, pp. 568-571.

[35] H. Suzuki, "A statistical model for urban radio propagation," *IEEE Trans. Commun.*, vol. 25, no. 7, pp. 673-680, July 1977.

[36] A. Abdi, W. C. Lau, M.-S. Alouini, and M. Kaveh, "A new simple model for land mobile satellite channels: first- and second-order statistics," *IEEE Trans. Wireless Commun.*, vol. 2, no. 2, pp. 519-528, May 2003.

[37] P. S. Bithas, N. C. Sagias, P. T. Mathiopoulos, G. K. Karagiannidis,and A. A. Rontogiannis, "On the performance analysis of digital communications over generalized-*K* fading channels," *IEEE Commun.Lett.*, vol. 10, no. 5, pp. 353-355, May 2006.

[38] A. Laourine, M.-S. Alouini, S. Affes, and A. Stéphenne, "On the capacity of generalized-*K* fading channels," *IEEE Trans. Wireless*

Commun., vol. 7, no. 7, pp. 2441-2445, Jul. 2008.

[39] S. Al-Ahmadi, H. Yanikomeroglu, "On the approximation of the generalized-*K* distribution by a Gamma distribution for modeling composite fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 706-713, Feb. 2010.

[40] I. M. Kostic, "Analytical approach to performance analysis for channel subject to shadowing and fading," *IEE Proc. Commun.*, vol. 152, no. 6, pp. 821-827, Dec. 2005.

[41] I.S.Gradshteyn and I.M.Ryzhik, Table of integrals, series and products. New York: Academic Press, 2007, 7th edn.

[42] M. Chiani, D. Dardari, and M. K. Simon, "New exponential bounds and approximations for the computation of error probability in fading channels," *IEEE Trans. Wireless Commun.*, vol. 2, no. 7, pp. 840-845, Jul. 2003.